UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,572	02/18/2004	Gary L. Graunke	42P17831	4741

45209   7590   02/01/2010

INTEL/BSTZ
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER
CALLAHAN, PAUL E

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
02/01/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *22 December 2009*.

2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-3,5-8,11-14,31-33,35 and 41* is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-3, 5-8, 11-14, 31-33, 35, and 41* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a) ☐ All   b) ☐ Some * c) ☐ None of:

　　　1. ☐ Certified copies of the priority documents have been received.

　　　2. ☐ Certified copies of the priority documents have been received in Application No. _____.

　　　3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   This Office Action is prompted by the Applicant's response filed 12-22-2009.

Claims 1-3, 5-8, 11-14, 31-33, 35, and 41 remain pending and have been examined.

Response to Arguments

2.   Applicant's arguments filed 12-22-2009 have been fully considered but they are

not persuasive.

The Applicant argues that the rejections of the claims under 35 USC Sec. 103(a)

are improper.

The Applicant argues that Best fails to teach the feature of a key update request

that is initiated by the chip receiving the key, or that the request must be authenticated.

The Examiner respectfully counters by noting that Best was not used to teach these

features in the rejections of the claims. Best (col. 14 lines 15-67 was used to teach the

feature of a key update request, not that the request is initiated by the chip. Ober was

used to teach such a step, wherein a secret key (a random number) is programmed into

a chip, and later a key request message is generated by the chip and a public/private

key pair is generated using the random number (fig. 1, col. 3 lines 1-40).

The Applicant argues that Hur fails to teach the feature of generation of a private

key for a manufactured chip in response to a key update request wherein the update

request must be authenticated. The Examiner respectfully counters that a review of Hur

reveals that such a feature of an authenticated key update request is taught at the cited

portions (Abstract, col. 6 lines 18-40, col. 10 lines 33-38). For example, Hur describes

such a process in his abstract section: "*The first device registers with the registration service and obtains a longer-lived symmetric key. Using the longer-lived key, the first device authenticates itself to a key management service, and receives a shorter-lived symmetric key encapsulated in a ticket that includes policy information*"

The Applicant argues that the rejection of claim 1 under 35 USC Sec. 103(a) is improper because Best fails to teach both programming of a chip secret key into a manufactured chip, and generating at least one private key for the manufactured chip in response to a received key update request. The Examiner respectfully counters that Best teaches both steps at the cited portions. Loading of a key into the chip is taught at col. 4 line 64: "*The key is loaded into CMP 16 via line 163 by unit 184 whose operation is described below*", at col. 7 lines 4-5: "*The cipher key may be stored into register 5 prior to distribution of CMP 16 to users*", and at col. 14 lines 52 and 53 where an operator may request that a second processor generate a key for the CMP chip and load it into memory.

The Applicant argues that Ober fails to teach the feature of generation of a private key for the chip. The Applicant asserts that Ober preferentially utilizes a Diffie-Hellman algorithm and therefore any authentication must involve the public key of the chip which by definition is disclosed. The Examiner respectfully disagrees with this characterization of Ober, and points out that Ober was used to teach only the feature of a key update request message that is initiated by the chip. Ober teaches this feature at the cited passages, and at col. 4 lines 30-36.

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

4.   Claim 6 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite

for failing to particularly point out and distinctly claim the subject matter which applicant

regards as the invention.

The first line of claim 6 reads: "The method of claim 1, wherein generating the

private further comprises:" The claim should read as to "wherein generating the private

<u>key</u> further comprises."

Double Patenting

5.   The nonstatutory double patenting rejection is based on a judicially created
doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the
unjustified or improper timewise extension of the "right to exclude" granted by a patent
and to prevent possible harassment by multiple assignees.   A nonstatutory
obviousness-type double patenting rejection is appropriate where the conflicting claims
are not identical, but at least one examined application claim is not patentably distinct
from the reference claim(s) because the examined application claim is either anticipated
by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140
F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29
USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir.
1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422
F.2d 438, 164 USPQ 619 (CCPA 1970); and In *re Thorington*, 418 F.2d 528, 163 USPQ
644 (CCPA 1969).
A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d)
may be used to overcome an actual or provisional rejection based on a nonstatutory
double patenting ground provided the conflicting application or patent either is shown to
be commonly owned with this application, or claims an invention made as a result of
activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6.   Claims 1-3, 5-8, 11-14, 31-33, 35 and 41 are provisionally rejected on the ground

of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-

29 of co-pending U.S. Patent Application Pub. No.2007/0223704 A1. Although the

conflicting claims are not identical, they are not patentably distinct from each other

because claims 1-29 of the co-pending U.S. Patent Application contain every element of

claims 1-3, 5-8, 11-14, and 31-35 of the instant application and as such anticipate the

claims of the instant application. This is a <u>provisional</u> obviousness-type double patenting

rejection because the conflicting claims have not in fact been patented.

"A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim. <u>In re Longi</u>, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); <u>In re Berg</u>, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus). " ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set
forth in section 102 of this title, if the differences between the subject matter sought to be patented and
the prior art are such that the subject matter as a whole would have been obvious at the time the
invention was made to a person having ordinary skill in the art to which said subject matter pertains.
Patentability shall not be negatived by the manner in which the invention was made.

8.   Claims 1, 11, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Best, US 4,278,837 (submitted with the Applicant's IDS), Ober et al., US

6,278,782, and Hur, US 7,181,620.

        As for claim 1, Best teaches a method comprising: programming a chip secret

key into a manufactured chip; sending the manufactured chip to a system original

equipment manufacturer (OEM) (fig. 1 element 5, fig. 2 element 5, 89, fig. 3 element

167, col. 4 lines 40-67, col. 7 lines 5-25); and generating at least one private key for the

manufactured chip according to a received key update request (col. 14 lines 15-67).

Best does not teach a step wherein the update request is made by the chip. However,

Ober does teach such a step, wherein a secret key (a random number) is programmed

into a chip, and later a key request message is generated by the chip and a

public/private key pair is generated using the random number (fig. 1, col. 3 lines 1-40).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to incorporate this feature into the system of Best. It would have

been obvious to do so since this would increase the security of key updates for a chip

by performing the update at a secure manufacturer facility. The combination of Best

and Ober fails to teach the step wherein the update request is authenticated, or that

the chip is enabled for authentication without disclosure of the private key or any

unique device identification information of the manufactured chip. However, Hur does

teach a system wherein a key update request is authenticated (Abstract, col. 6 lines

18-40, col. 10 lines 33-38), and that authentication can take place without disclosure

(fig. 7, fig. 8, col. 10 lines 15-55). Therefore, it would have been obvious to one of

ordinary skill in the art at the time the invention was made to incorporate this feature

into the system of Best. It would have been obvious to do so since this would increase

the security of key updates for a chip.

Claims 11 and 31 are directed towards the computer-program product that

instructs a processing system to carry out the method of claim 1. Claim 31 represents

the apparatus utilizing the method of claim 1. Claims 11 and 31 recite substantially the

same limitations as claim 1 and are rejected on the same basis as that claim.

Allowable Subject Matter

9.   Claims 2, 3, 5-8, 12-14, 32, 33, 35, and 41 would be allowable if rewritten in

independent form including all of the limitations of the base claim and any intervening

claims, and if a Terminal Disclaimer directed towards U.S. Patent Application Pub.

No.2007/0223704 A1.

Conclusion

10.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

11.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-

3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's

supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is: (571)

273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

/PEC/
AU2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437